



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/037,511	01/04/2002	Andrew Brown	COMP.0268 P01-3942	6225

7590 05/16/2005

Intellectual Property Administration
Legal Dept., M/S 35
P.O. Box 272400
Ft. Collins, CO 80527-2400

EXAMINER

SHIFERAW, ELENI A

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 05/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/037,511

Applicant(s)

BROWN ET AL.

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 1/4/2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 04 January 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>4/15/2002</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-20 are presented for examination.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, and 7-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsao et al. (Tsao, Pub. No.: 2002/0087857 A1) in view of Utz (Patent Number: 6,097,307).

As per claim 1, Tsao teaches a method of ensuring a random number for a cryptographic security subsystem of a processor-based device, the method comprising the acts of:

obtaining a seed pool comprising a plurality of bits for generating the random number (Tsao fig. 2 No. 16a);

remotely storing a seed pool backup of the seed pool via a network (Tsao page 4 par. 0077 lines 7-10); and

Tsao does fail to teach restoring the seed pool backup to local memory following a power loss event causing loss to the seed pool.

However Utz teaches restoring the seed pool backup to local memory following a power loss event causing loss to the seed pool (Utz abstract lines 10-13; pseudo random number generator generates a another pseudo-random number if power to the transmitting unit is interrupted).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Utz within the system of Tsao because it would allow to restore a new random number when removing and replacing battery or when power is interrupted (Utz abstract lines 10-13).

As per claim 7, Tsao, and Utz, teach all the subject matter as described above. In addition Utz teaches the method, wherein the act of restoring the seed pool backup comprises the act of automatically retrieving the seed pool backup via the network upon restoring power to the cryptographic security subsystem (Utz abstract lines 10-13).

As per claim 8, Tsao, and Utz, teach all the subject matter as described above. In addition Utz teaches the method, wherein the act of automatically retrieving the seed pool backup comprises requesting the seed pool backup from a remote management system (Utz abstract lines 10-13).

As per claim 9, Tsao, and Utz, teach all the subject matter as described above. In addition Utz teaches the method, wherein the power loss event is a battery failure resulting in memory loss of the seed pool from the local memory (Utz abstract lines 10-13).

As per claim 10, Tsao, and Utz, teach all the subject matter as described above. In addition Utz teaches the method, wherein the act of restoring the seed pool backup comprises the act of transmitting the seed pool backup from remote storage to the local memory via the network following a battery replacement for the local memory (Utz abstract lines 10-13).

4. Claims 11, and 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Liu et al. (Liu, Patent No.: US 6,760,752 B1), in view of Utz (Patent Number: 6,097,307).

As per claim 11, Liu teaches a method of restoring a seed pool for generating a random number for a security system, the method comprising the acts of:

transmitting a periodically stored backup of the seed pool to the security system via a network (Liu col. 30 lines 45-47); and

Liu does not explicitly teach local memory of the security system with the periodically stored backup for use in generating the random number following loss of the seed pool from the security system;

However Utz discloses repopulating local memory of the security system with the periodically stored backup for use in generating the random number following loss of the seed pool from the security system (Utz abstract lines 10-13; pseudo random number generator generates a another pseudo-random number if power to the transmitting unit is interrupted).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Utz within system of Liu because it would

Art Unit: 2136

allow to restore a new random number when removing and replacing battery or when power is interrupted (Utz abstract lines 10-13).

As per claim 14, Liu and Utz teach all the subject matter as described above. In addition, Liu teaches the method, comprising the act of periodically storing the seed pool in a remote storage device via the network at an interval based on a write cycle characteristic of the remote storage device to maintain availability of the seed pool as the periodically stored backup (Liu col. 30 lines 45-55). The rationale for combining are the same as claim 11 above.

As per claim 15, Liu and Utz teach all the subject matter as described above. In addition Utz teaches the method, wherein the act of transmitting the periodically stored backup comprises the act of transferring the periodically stored backup to the security system after restoring battery power to the security system (Utz abstract 10-13).

As per claim 16, Liu and Utz teach all the subject matter as described above. In addition Utz teaches the method, wherein the act of transferring the periodically stored backup comprises automatically initiating a seed pool restoration event using the periodically stored backup stored on a remote server after restoring battery power by replacing a battery for the local memory of the security system (Utz abstract 10-13).

Art Unit: 2136

5. Claims 17-18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsao et al. (Tsao, Pub. No.: 2002/0087857 A1) in view of Liu et al. (Liu, Patent No.: US 6,760,752 B1), and Utz (Patent Number: 6,097,307).

As per claim 17, Tsao teaches a security system, comprising:

- a security subsystem, comprising:

- a power dependent memory device (Tsao page 4 par. 0077 lines 7-10, and par. 0081 lines 1-5);

- a limited life battery for the power dependent memory device (Tsao page 4 par. 0077 lines 7-10, and par. 0081 lines 1-5);

- a seed pool stored on the power dependent memory device, wherein the seed pool comprises a plurality of random bits (Tsao page 4 par. 0077 lines 7-10, and par. 0081 lines 1-5); and

- security logic configured to generate a cryptographic key to establish a secure communication session between the electronic device and an external device, wherein the security logic generates the cryptographic key from the seed pool (Tsao page 4 par. 0093, page 1 par. 0010; Random number generator generates encryption and decryption key based on random number); and

- a security backup system, comprising:

- a remote storage device (fig. 3 No. 16, page 4 par. 0076);

Tsao does not explicitly teach a backup control module configured for periodically storing a backup of the seed pool in the remote storage device;

However Liu teaches teach a backup control module configured for periodically storing a backup of the seed pool in the remote storage device (Liu col. 30 lines 45-47);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Liu within the system of Tsao because it would enhance security by periodically generating and transmitting random number to the remote client and make the security system difficult to the third person to retrieve keys every minute.

Tsao and Liu do not explicitly teach replacement of limited life battery.

However Utz discloses a restoration control module configured for repopulating the power dependent memory device with the backup following replacement of the limited life battery (Utz abstract lines 10-13; pseudo random number generator generates a another pseudo-random number if power to the transmitting unit is interrupted).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Utz within the combination system of Tsao and Liu because it would allow to restore a new random number when removing and replacing battery or when power is interrupted (Utz abstract lines 10-13).

As per claim 18, Tsao, Liu and Utz teach all the subject matter as described above. In addition Utz teaches the method, comprising a remote security interface configured for interacting with the security subsystem and the security backup system (Utz abstract lines 10-13). The rational for combining are the same as claim 17 above.

As per claim 20, Tsao, Liu and Utz teach all the subject matter as described above. In addition Utz teaches the method, wherein the security backup system comprises an automation module configured for automatically initiating repopulation of the memory device with the backup (Utz abstract lines 10-13). The rational for combining are the same as claim 17 above.

6. Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsao et al. (Tsao, Pub. No.: 2002/0087857 A1) in view of Utz (Patent Number: 6,097,307), and further in view of Liu et al. (Liu, Patent No.: US 6,760,752 B1).

As per claim 2, Tsao and Utz teach all the subject matter as described above.

Tsao and Utz fail to explicitly teach the act of periodically storing the seed pool back up.

However Liu teaches the method, wherein the act of remotely storing the seed pool comprises the act of periodically storing the seed pool backup on a remote storage device (Liu col. 30 lines 45-55).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Liu within the combination system of Tsao and Utz because it would enhance security by periodically generating and transmitting random

number to the remote client and make the security system difficult to the third person to retrieve keys every minute (Liu col. 30 lines 45-55).

As per claim 3, Tsao, Utz and Liu teach all the subject matter as described above. In addition Liu teaches the method, wherein the act of periodically storing the seed pool backup comprises the act of executing a backup event at a backup interval based on a write cycle characteristic of the remote storage device (Liu col. 30 lines 45-55). The rationale for combining are the same as claim 2 above.

7. Claims 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsao et al. (Tsao, Pub. No.: 2002/0087857 A1) in view of Utz (Patent Number: 6,097,307), Liu et al. (Liu, Patent No.: US 6,760,752 B1), and Gallup et al. (Gallup, Patent Number: 5,258,936).

As per claims 4, Tsao, Utz and Liu teach all the subject matter as described above. Tsao, Utz and Liu fail to teach modifying the seed pool backup with additional random bits to ensure randomness for generating the random number.

However Gallup teaches the method, comprising the act of modifying the seed pool backup with additional random bits to ensure randomness for generating the random number (Gallup abstract lines 4-8).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Gallup within the combination system of

Tsao, Utz and Liu because it would increase the randomness of the pseudo-random numbers (Gallup abstract lines 4-8).

As per claim 5, Tsao, Utz, Liu, and Gallup teach all the subject matter as described above. In addition Gallup teaches the method, wherein the act of modifying the seed pool backup with additional random bits comprises the act of capturing one or more bits of data from a free-running timer (Gallup abstract lines 4-8). The rationale for combining are the same as claim 4 above.

As per claims 6, Tsao, Utz, Liu, and Gallup teach all the subject matter as described above. In addition Gallup teaches the method, wherein the act of modifying the periodically stored backup with additional random bits comprises the act of capturing one or more bits of data from one or more local hardware components (Gallup abstract lines 4-8). The rationale for combining are the same as claim 4 above.

8. Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Liu et al. (Liu, Patent No.: US 6,760,752 B1), in view of Utz (Patent Number: 6,097,307), and further in view of Gallup et al. (Gallup, Patent Number: 5,258,936).

As per claims 12, Liu and Utz teach all the subject matter as described above. Liu, and Utz fail to teach modifying the seed pool backup with additional random bits to ensure randomness for generating the random number.

However Gallup teaches the method, comprising the act of modifying the seed pool backup with additional random bits to ensure randomness for generating the random number (Gallup abstract lines 4-8).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Gallup within the combination system of Liu and Utz because it would to increase the randomness of the pseudo-random numbers (Gallup abstract lines 4-8).

As per claims 13, Liu, Utz, and Gallup teach all the subject matter as described above. In addition Gallup teaches the method, wherein the act of modifying the periodically stored backup with additional random bits comprises the act of capturing one or more bits of data from one or more local hardware components (Gallup abstract lines 4-8). The rational for combining are the same as claim 12 above.

9. Claims 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tsao et al. (Tsao, Pub. No.: 2002/0087857 A1) in view of Liu et al. (Liu, Patent No.: US 6,760,752 B1), and Utz (Patent Number: 6,097,307), and further in view of Gallup et al. (Gallup, Patent Number: 5,258,936).

As per claim 19, Tsao, Liu, and Utz, teach all the subject matter as described above.

Liu and Utz do not explicitly tech modification module configured for capturing one or more bits of data from a hardware component and adding the one or more bits to the backup.

Art Unit: 2136

However Gallup teaches the method, wherein the security backup system comprises a seed pool modification module configured for capturing one or more bits of data from a hardware component and adding the one or more bits to the backup (Gallup abstract lines 4-8).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Gallup within the combination system of Tsao, Liu and Utz because it would to increase the randomness of the pseudo-random numbers (Gallup abstract lines 4-8).

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867.

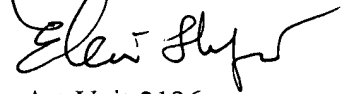
The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

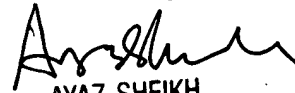
Eleni Shiferaw

Art Unit: 2136



Art Unit 2136

May 5, 2005



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100